Make-or-Break Phishing Metrics

How to measure and drive behavior change that shields your organization from cyber-attacks

EMPLOYEES AND THEIR MAILBOXES ARE YOUR GREATEST CYBERSECURITY RISK FACTOR. HOXHUNT RECENTLY ANALYZED 24.7 MILLION PHISHING SIMULATIONS ACROSS 1.6 MILILION USERS. THE FINDINGS UNDERSCORE THE IMPORTANCE OF FOUR KEY METRICS NEEDED TO LIMIT TRUE RISK.

Failure rate

% OF USERS WHO FALL FOR A SIMULATED ATTACK

DON'T PUNISH!

Users who feel singled out for making mistakes will disengage. Building a human firewall against phishing attacks requires everyone's participation.

INSTEAD

MAKE IT POSITIVE AND FUN

Use easily digestible microtraining followed by simpler simulations to develop skills over time. By putting each individual on a gamified learning journey, you'll turn critics into contributors and build resilience one user at a time.

Success Rate

% OF USERS WHO REPORT A SIMULATED PHISHING EMAIL

INSTEAD

DON'T MAKE REPORTING DIFFICULT!

Most companies struggle here. Forgettable instructions and cumbersome processes make it hard to report and track simulated phishes. That keeps people from learning behaviors that will protect the organization.

MAKE IT EASY AND REWARDING

Use game mechanics to encourage active reporting behavior. Give positive reinforcement to build skills. Never stop training: continue challenging users with more difficult simulations.

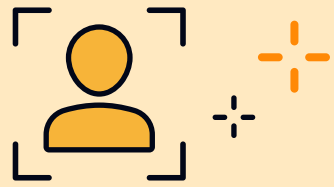
Miss rate

% OF USERS WHO DIDN'T RESPOND TO A SIMULATION (I.E., NEITHER FAILED NOR SUCCEEDED)

DON'T CELEBRATE!

Not failing isn't success! Your "missers" (users who neither fail nor succeed) lack the skills to spot real attacks. They're missing pieces of the human firewall needed to protect your company.

INSTEAD

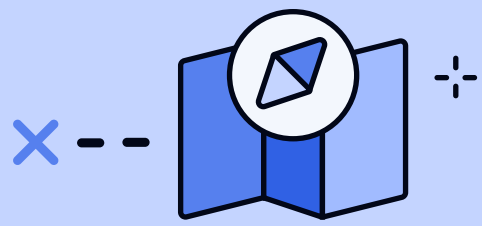


FOCUS ON YOUR "MISSERS"

Use every awareness tactic possible to engage them. Simulation success and failure are preferable. Why? Because both lead to positive microtraining moments that will build resilience.

Real Threat Reporting Rate

RATE AT WHICH USERS NOTIFY IT ABOUT SUSPICIOUS, NON- SIMULATED EMAILS



DON'T LOSE SIGHT OF THE GOAL!

Too many companies see reporting of real phishes as a "maybe someday" target. But every day that real threats go unreported is a day of serious risk to your organization.

INSTEAD

GET IN FRONT OF REAL THREATS TODAY

Use the same process for reporting real and simulated threats. You'll hardwire instinctive behaviors that will give IT early warnings of real-world attacks.

HOXHUNT

Hoxhunt helps to educate employees on email-based threats, such as phishing, so that they can learn to recognize and report real attacks. With Hoxhunt, you can build a strong human firewall to protect your organization from cyber attacks.

HOXHUNT.COM

Download the free Behavioral Cybersecurity Report here